

GDIT HFPP Trusted Third Party Information System

Work Aid - Secure Account Management Processes

This reference outlines the key account management steps in the system user lifecycle for all TTP system users. These steps align with security practices required to safeguard the information system and its data assets.

Note: A separate, role-based mapping of HFPP Partner-specific processes is provided in

Table 2: TTP Security - HFPP Onboarding and Access and Table 3: TTP Security - HFPP Offboarding and Deactivation.

Table 1: Summary - User Lifecycle Account Management Sequence

***Detail about process implementation is not included in this document.*

Step	HFPP Partner	Other TTP Personnel Users
1	<p>ONBOARDING AND ACCESS</p> <p>HFPP Partner selection and approval processes are completed.**</p> <p>Partner candidate sends formal request for HFPP membership.**</p>	<p>ONBOARDING AND ACCESS</p> <p>TTP employee new hire selection and acceptance is completed.</p> <p>Newly-hired TTP employee completes all required corporate (primary) / subcontractor legal and related documentation. (Includes TTP PMO documentation for new staff.)</p>
2	<p>New Partner introduced to the Memorandum of Understanding (MOU) and Data Sharing Agreement (DSA) documents.</p>	<p>New TTP employee information system role and type is determined to coordinate system accesses: <i>Two general TTP access types identified for Admins/Developers and Analysts.</i></p>

Step	HFPP Partner	Other TTP Personnel Users
3	Executed MOU/ DSAs stored on SharePoint.	New TTP employee completes security and related agreements (RoB & others) required for system access types.
4	Once MOU is executed: A: HFPP Partner Orientation Meeting held. B: New Partner identifies POC and additional Portal users. C: Request made for new user access to TTP Portal for new Partner.	Information system/Portal and other relevant training provided.
5	A: Meeting follow-ups held to support new Partner in completing DSA.	Once agreements/training complete, Tech Mgr. is notified. System accesses implemented for Admins/Developers and Analysts, accordingly.
6	B, C: Once IT receives new user access request for new Partner, the new Partner POC identity is verified.	<i>For new Admins/Developers:</i> System tickets opened/corporate cloud services requested for VPN access (to the TTP system).
7	Once the new Partner POC/new system user is verified through appropriate program processes, the new user system role and type is determined.	Once new TTP employee accesses established, tickets closed.
8	Add user form is created / new user registered.	
9	Registration data sent to Portal, which sends to Microsoft Active Directory (AD) where the data is received/stored. Receipt of registration data triggers Portal account activation email.	
10	Portal account activation email sent to new user.	

Step	HFPP Partner	Other TTP Personnel Users
11	New user receives Portal account activation email; clicks link to take security training and begin Symantec VIP (VIP) access process.	
12	New user presented with registration screens; proceeds through VIP access process and completes as instructed.	
13	Portal receives confirmation that VIP process is complete; presents Create Password form.	
14	New user completes Create Password form.	
15	New user data processed by AD and rejected/verified for storage and confirmation with the Portal. (If AD rejects user data, step is restarted, "Portal account activation email sent to new user.")	
16	AD approves password; sends confirmation to Portal.	
17	Secure sign-in page presented to new user.	
18	New user signs in with new password; Portal Dashboard page or Portal main menu landing page is presented. TTP system access is complete.	
19	(COMMON PROCESS) ACCOUNT MONITORING AND REVIEW IT team identifies privileged and nonprivileged user accounts types and establishes a monitoring schedule for each type.	
20	Assigned IT team members review each account type on the designated schedules.	
21	IT team member documents the results of the review of user account status and takes any appropriate action, as required.	